

Strategy Session

Mobility 101: Surviving The 'BYOD' Revolution

End-user demands for a wider selection of smartphones and tablets—including the option to connect their own devices to the corporate network—are gaining traction. Gone are the days when smartphones were corporate-provided assets and IT managers could dictate the device (typically a BlackBerry) and enforce policies to ensure total management and security for enterprise data. Now what?

By Michael Finneran



Strategy Session

T A B L E
O F
C O N T E N T S

3	Author's Bio
4	No Stemming This Tide
4	Figure 1: Organizational Approach to Consumer-Centric Technology
5	The No Police?
5	It All Starts With a Mobility Policy
6	Figure 2: Increase in Employee-Owned Mobile Devices?
9	Figure 3: Mobile Device and Data Policies?
10	Figure 4: Securing End-User Devices
13	Figure 5; Prioritization of Mobile Data Security
14	Putting the Plan Into Action
15	Figure 6: Custom Business Applications for Mobile Devices
16	Catch Up
17	Related Reports

ABOUT US | *InformationWeek's* experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption Strategy Session gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at awittmann@techweb.com, content director **Lorna Garey** at lgarey@techweb.com and research managing editor **Heather Vallis** at hvallis@techweb.com. Find all of our reports at www.analytics.informationweek.com.



Strategy Session

**Michael
Finneran**
InformationWeek



Michael Finneran is an independent consultant and industry analyst specializing in wireless technologies, mobile unified communications and fixed/mobile convergence. He has more than 30 years in the networking field and is the author of *Voice Over Wireless LANs: The Complete Guide* (Elsevier, 2008). His expertise spans the full range of wireless technologies, including Wi-Fi, 3G/4G cellular, WiMax and RFID.

In the consulting area, Michael has provided assistance to carriers, equipment vendors, end users and investment firms in the United States and overseas. He has appeared at hundreds of trade shows and industry conferences, including Enterprise Connect (formerly VoiceCon) and Interop; he now serves as the program chair for wireless and mobility at Enterprise Connect.

Michael is also prolific writer; for 23 years he wrote the Networking Intelligence column for *Business Communications Review*. He now contributes on wireless and mobility to numerous publications. As an educator, he has conducted more than 2,000 seminars on networking topics globally, including the graduate telecommunications program at Pace University and programs at the Center for the Study of Data Processing at Washington University in St. Louis. His programs are now offered through Telecom+UC Training. A longtime member of the Society of Telecommunications Consultants, Michael holds a master's degree in marketing and management information systems from the J.L. Kellogg Graduate School of Management at Northwestern University.



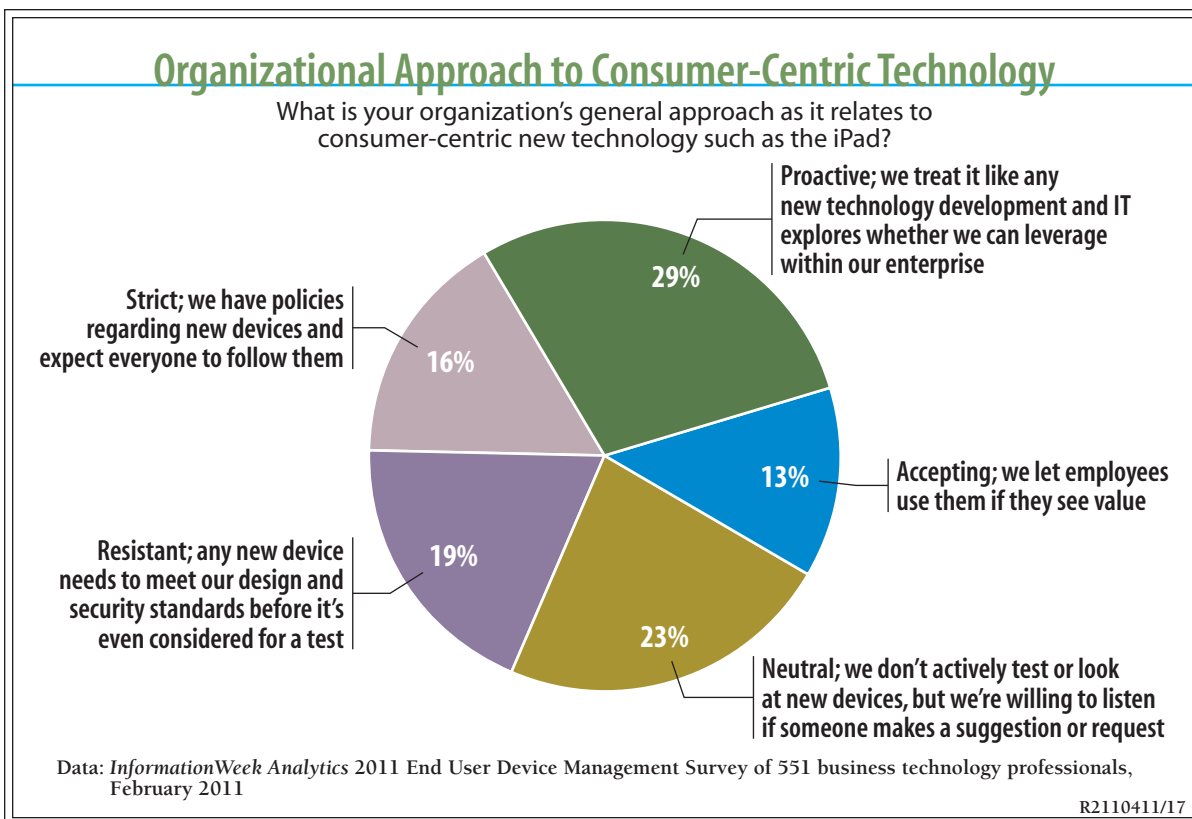
Strategy Session

No Stemming This Tide

Information security teams are scrambling to protect roving users connecting to the corporate network via personal devices outside IT's control. Seems like mission impossible, but we have no choice. Smartphones have gone from being a high-end corporate perk to a wildly successful consumer product. IDC expects total smartphone sales in 2011 to reach 472 million across the globe, rising to 982 million in 2015. A recent study by Nielsen found that 55% of new handset sales in the United States are now smartphones, up from 34% a year ago. During that same period, RIM's share of U.S. smartphone sales has fallen to 21%, while Android sits at 38% and Apple iOS at 27%. And don't forget tablets: Caris & Co. predicts that sales of Apple's iPad, the dominant option in this market, will grow from 14 million in 2010 to 36 million in 2011.

Meanwhile, our *InformationWeek* 2011 End User Device Management Survey of 511 business technology professionals found that organizations are warming up to the idea of welcoming

Figure 1



**S t r a t e g y S e s s i o n**

consumer-centric technologies such as the iPad onto their networks. Some 42% identified their organizational approach as either “accepting” or “proactive,” while 23% ranked themselves “neutral”; the remaining 35% still peg their posture as “resistant” or “strict.”

Good luck with that stance once the business realizes how much money could be saved by letting employees buy their own devices and data plans, not to mention the productivity gains.

The No Police?

The scenario: Your company’s new CMO just called. She wants to use her iPhone to get her corporate email. Could you send someone up to help configure it? Oh, and by the way, her assistant has an Android phone, and he’ll need mail access set up as well.

Now, the two smartphone platforms have different profiles relative to malware, both can make use of open Wi-Fi hotspots—and both will store sensitive product information. A flat-out “no” won’t win you any friends, but just granting access with no controls and exposing corporate information to loss or theft will put you in an even worse position. We need a middle ground. In this Strategy report, we’ll lay out the seven areas you must address in your mobility policy. We’ll also discuss how to identify potential vulnerabilities, investigate your management and security options, and get a plan together—before you find your back against the wall.

It All Starts With a Mobility Policy

The plain truth of the matter is that unless you have a written mobility policy that is endorsed and supported by management, there’s no such thing as right or wrong. If you don’t already have a policy, it’s time to get to work. If you do, it probably doesn’t cover the bring-your-own-device (BYOD) option, so it’s time for an update.

The first thing to realize is that many of the elements you need to include go beyond IT’s purview. Line-of-business and executive managers are not likely to recognize what’s at stake, so a key task will be education, and that means initiating a constructive dialogue tailored to your industry. Managers in regulated sectors such as banking and healthcare will be well aware of compliance issues and, we find, are adept at describing what’s at stake when employees start using their own smartphones and tablets. In other industries, where security has not been such a core focus, it may take some work to raise the awareness level.

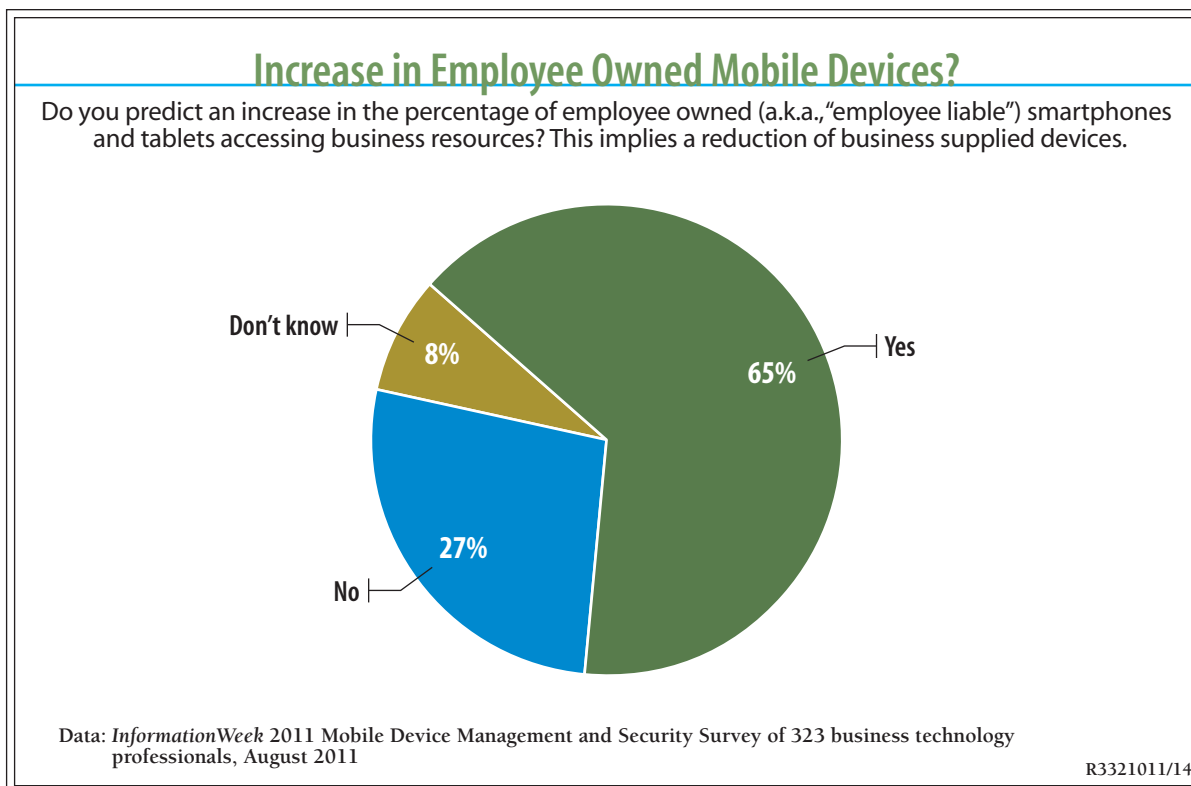


Strategy Session

Elements you should bring up include:

- The possibility of sensitive emails, contacts, product plans or technical information falling into the wrong hands if a device is lost or stolen or if an attacker can gain access over an unsecured connection.
- Employees leaving the company with that information still intact on their mobile devices.
- Malware that infects the mobile device itself.
- The possibility of introducing viruses or malware collected on the mobile device into the wired network and back-office systems.
- The use of unauthorized software that exposes other information on that device to outsiders, or the cost of network services run up by that rogue application.

Figure 2



**S t r a t e g y S e s s i o n**

- The loss of control of contact numbers, so when employees leave the company, customers and prospects continue to contact them at their mobile numbers.
- The time and cost involved in recovering information for a mobile device that has not been routinely backed up.
- The cost of providing help desk support to a half-dozen different mobile operating systems.
- Applications—who decides what can be installed, and from what sources? Will the company have an “app store” to deliver mobile versions of business applications?
- Today’s mobile device management systems come with a huge range of options: device lock-outs, Wi-Fi policies, the ability to wipe lost phones, application black- and whitelists. Who decides on company standards?
- The potential liability to the company if an employee injures someone while talking on a business call while driving—with or without a headset.

You can probably come up with additional items based on the nature of your business.

The idea of a mobility policy is to set out the basic ground rules that will govern the provisioning and use of mobile devices and services, including the definition of acceptable use, user responsibilities and penalties for repeated noncompliance. Our *InformationWeek* 2011 Mobile Device Management and Security Survey, which we limited to respondents at companies with 50-plus employees involved with determining mobile/wireless strategy or evaluating, recommending or purchasing mobile devices, shows fewer than half have written policies and procedures pertaining specifically to mobile/portable devices or the handling of mobile data. Meanwhile, 65% predict an increase in the percentage of employee-liable smartphones and tablets accessing business resources.

And many times, we see that even in companies with policies, employees feel under no obligation to comply.

The first step in developing a workable and enforceable mobile policy is to define who will be responsible for maintaining and enforcing it. We believe that day-to-day responsibility should

**S t r a t e g y S e s s i o n**

be with the IT organization, and we most often see executive control reside with the CIO or CFO. The biggest overall questions to address are these: Who's entitled to a device? Who's going to pay for it? What range of devices are you going to support and to what extent? What are the user's responsibilities? What are the penalties for noncompliance? Let's take a closer look at each of these.

1. Who should get a company-owned mobile device or a stipend to buy one?

Most likely, not everyone. This decision should be based on role and spelled out clearly. The policy should also specify what type of device and service plan (voice or data or both) are authorized for each specific job title and who has the authority to overrule the policy.

2. Who pays?

Mobile devices for business have traditionally been provided and paid for by the company—the traditional “corporate-liable” model. But now we have to specify if BYOD is allowed, and if so, what the reimbursement policy will be. One major attraction of a corporate-liable plan is that we can typically negotiate better rates and terms than an off-the-street consumer. This is a tricky area, as setting the reimbursement rate too low may be seen as penalizing employees (particularly if the company had provided phones in the past) and lead to low morale. Further, if it's a corporate-paid phone, are personal voice and data use allowed, and at what point is it considered excessive? As unlimited data plans become rarer, this will become more of an issue.

So while cost savings are often cited as a benefit of BYOD, it will be important to get human resources to weigh in on what could potentially affect employee retention.

3. What mobile ecosystems (RIM, iOS, Android, Windows Phone 7) will IT support?

This is where things really get tricky, because not all mobile operating systems are created equal. For example, BlackBerry is still the standard for mobile security and typically the only option that is inherently FIPS 140-2 compliant.

Apple has made great strides in security with iOS 4.2. The Android 2.x releases and Windows Phone 7, on the other hand, do not support onboard encryption, creating a significant security threat if the device is lost or stolen (some third-party vendors are planning to introduce encryption capabilities for Android).



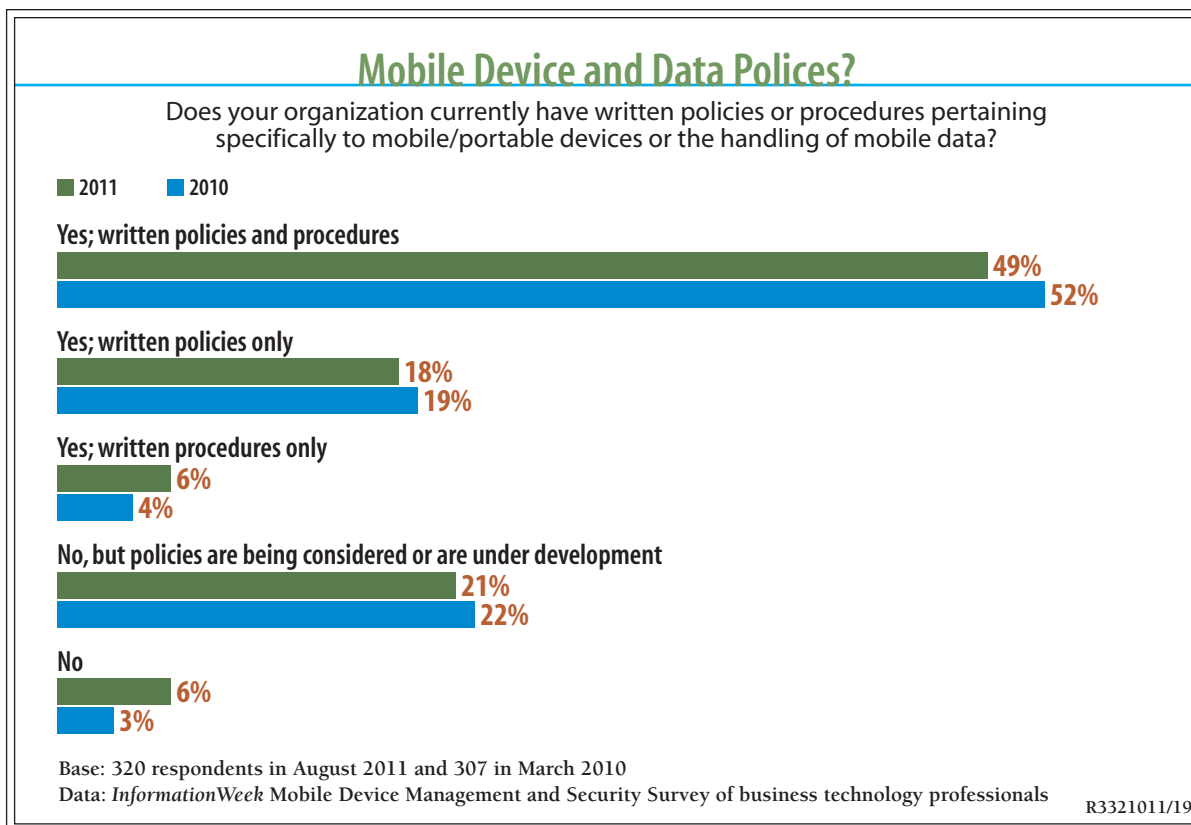
Strategy Session

And this fall, we'll see all new revs of these platforms. The capabilities of mobile operating systems improve on an erratic schedule, and there's a good chance Android will come to at least iPhone's level of security within the next 12 to 18 months. Android 3.0, which is used on tablets such as the Motorola Xoom, does feature onboard encryption, and it will likely be included in the next major release, Android 4.0 (a.k.a. "Ice Cream Sandwich").

In the meantime, a half-dozen Android releases are in circulation. This continuously evolving environment means IT should specify both the operating systems and version levels that are allowed and define a procedure for testing and certifying new devices, platforms and releases.

Finally, address precautions laptops, tablets and smartphones must employ when using potentially insecure Wi-Fi hotspots, or DECT or other proprietary wireless technologies.

Figure 3





Strategy Session

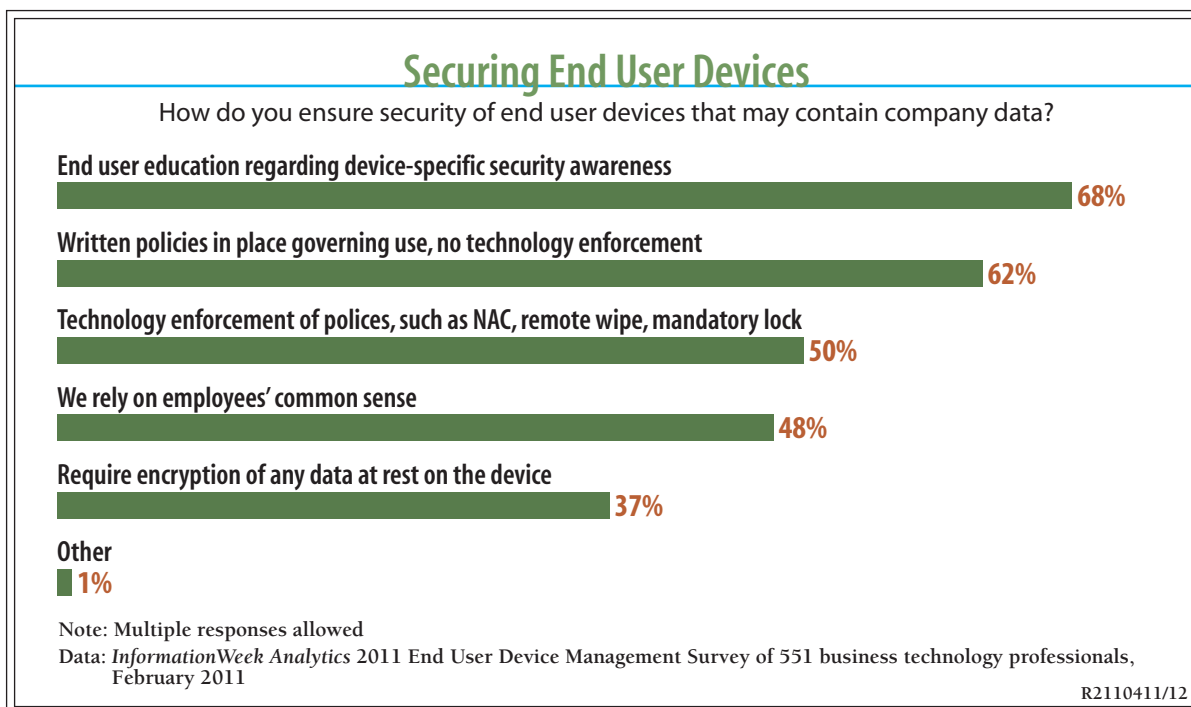
4. Are you going to provide support?

Once you know *what* you'll be taking responsibility for, you'll have to figure out *how* to do the job. This is where mobile device management, or MDM, systems such as those from AirWatch, MobileIron, Sybase (now part of SAP) and Zenprise come into the picture. As we discuss in our Mobile Device Management Buyer's Guide, interest in these products is booming as a result of BYOD, but you need to know what you're looking for before you go shopping, particularly with regard to the functions and operating systems supported.

Our Mobile Device Management and Security Survey showed dramatic movement when we asked about mobile device platform standardization. In our March 2010 poll, 73% said they standardized, and the IT department was responsible for procuring devices and carriers. By August 2011, just 58% answered that way, a 15-point drop.

However, our End User Device Management Survey found that only 50% of respondents had technology-based security enforcement. We did not break results out by OS, but there's a good chance that most of those systems are based on BES, which for now is BlackBerry only. Note

Figure 4





Strategy Session

that RIM has announced that, with the acquisition of MDM supplier Ubitexx, it will soon begin supporting iOS and Android devices through a shared BES interface.

MDM capabilities vary widely, but generally you will find policy enforcement (for example, the ability to require strong power-on passwords and on-device encryption if available in the OS and to enforce white- and blacklisted applications), and remote wipe and lock are standard. Many also feature internal app stores, troubleshooting and help desk tools, service monitoring and a raft of other capabilities.

Most of these systems require that a client be installed on the mobile device, so you also need to define the procedure to install the client and activate the user on the system (most support over-the-air device initiation). But be clear about which releases are supported, as your “power users” will want to update to the most recent release as soon as it’s available. Finally, figure out how to get the client off the device if the user leaves the company—after you’ve wiped corporate data, of course.

5. Do we need to control contact numbers?

An often overlooked security issue is the telephone number itself. For some organizations, contact numbers are an important corporate asset, and in customer-facing roles such as sales or service and support, it’s important that the company retain the number if the user leaves.

There are a number of technical and procedural alternatives here. The easiest is issuing a corporate-liable phone. If a saleswoman wants to use her existing personal number, you might have her sign a document asserting that the number becomes the property of the company and must be surrendered when she leaves. If that’s a hard sell, many PBX vendors offer clients that will route inbound and outbound business calls through the PBX, so the user can give her desk phone number to business contacts, and those calls will automatically be forwarded to her mobile. Outbound mobile calls are also routed through the PBX, and the caller ID provided to the business contact is the user’s desk number. The problem is that these setups require that the user employ a rather awkward mobile client for all business calls, and we have seen significant push-back as a result.

Of course, it’s usually a less unpleasant option than surrendering a phone number.

**S t r a t e g y S e s s i o n****6. What about training, responsibilities and penalties for noncompliance?**

The user is always the weak link in any security plan, so we must identify how people will be trained, how IT will let them know what is acceptable and unacceptable, their role in securing company information and minimizing liability, and the consequences should they fall short.

One very important provision will involve use while driving. Most organizations endorse what is “legally acceptable”; for example, you can talk while driving, but only if using a hands-free device when required by state law. Hands-free or not, though, if an employee injures someone while engaged in a business call, the victim will very likely sue the company—regardless of who owns the phone. “This is an issue juries can understand,” says telecom attorney Martha Buyer.

Consider asking your legal department whether a provision that bans all electronic device use while driving is in order. If you do put such a rule in place, be prepared for some serious push-back from your mobile workers. However, having a signed form that states your policy may be a lifesaver in litigation.

“Acceptable use” should spell out obvious things, like prohibiting harassing calls, but it should also specifically prohibit actions like jailbreaking (Apple) or rooting (Android) the mobile device. Jailbreaking or rooting the device allows unauthorized—and potentially malware-infected—applications to be installed. Spell out what these security exposures are, in terms users understand. Acceptable levels of personal voice and data use should also be specified, as well as procedures for when users travel internationally.

One headache that has been eliminated is the need to track the cost of personal phone calls made on company-owned devices. Until late last year, the IRS categorized cellphones as “listed property,” essentially the same designation as company cars. That meant that personal use had to be tracked and the cost added to the employee’s taxable income. While few companies bothered to do this, the IRS, particularly the arm that tracks nonprofits, did enforce the requirements and levied fines as high as \$239,000 on some universities.

Finally, come up with reasonable penalties for employees who consistently fail to follow the rules. Those penalties can escalate for repeat offenders and typically start with a warning, followed by loss of mobile privileges for some period of time. They could go so far as termination for users who willfully and repeatedly put company information at risk.



Strategy Session

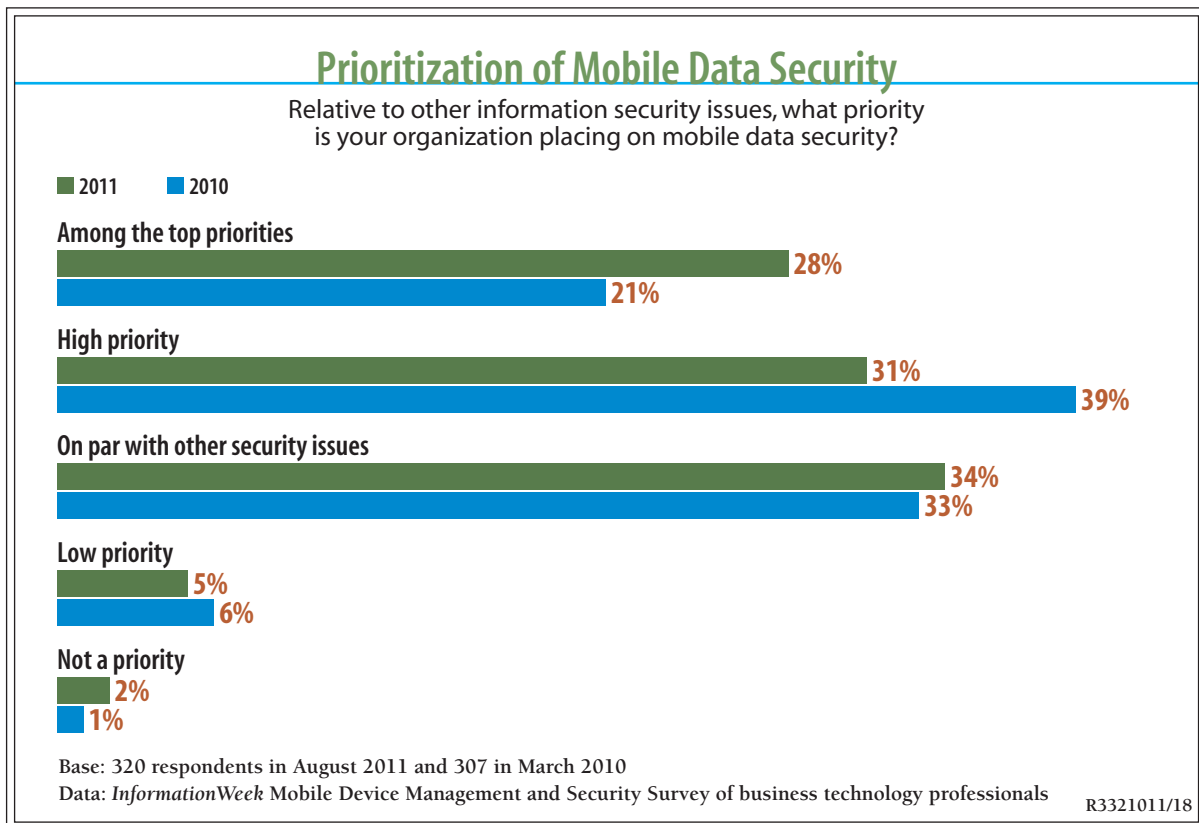
Needless to say, human resources will need to be consulted.

The last step of the process is to have employees sign a document that acknowledges that they have been informed of the rules, requirements and penalties. Further, if the policy is changed at a later date, everyone will need to confirm their understanding of the new rules.

7. How often do we revisit this policy?

The mobile business continues to evolve, with new devices, services, applications and challenges coming online all the time. Routine updates, such as adding support for additional devices, should not necessitate a full revision of the policy. We recommend, given the current pace of change, a yearly review cycle for the mobility policy; that review will also give you the opportunity to assess issues, exemptions and problem cases that have arisen.

Figure 5





S t r a t e g y S e s s i o n

Putting the Plan Into Action

Let's dig deeper into three hot-button areas: ownership, support and applications.

Ownership: Many organizations still look at mobility as a cost and manage it through purchasing or accounting. With the move to smarter devices; a fast-expanding selection of mobile applications; and increased need for security, support and management, mobility clearly belongs in IT. There is a cost element involved (and a growing one), so expense management and plan optimization should not be overlooked, but mobility is an enabling technology, and that should be the primary focus.

Define who is in charge of enterprise mobility. Note we said "mobility," not "cellphones." All wireless technologies offer the potential to increase efficiency, responsiveness and productivity, so "mobility" should be a broad technology umbrella. The mobility manager will have the day-to-day responsibility of maintaining and enforcing policies and working with carriers and local mobility coordinators at branch offices to see those policies are carried through. They will also interface with corporate security. As to resources, the mobility manager must have the budget to test and certify new devices and operating systems, to determine if they'll be supported. Further, the mobility manager will be responsible for expense management, plan optimization and negotiating service contracts.

Support: IT must stay engaged with mobile users. MDM systems will provide the technical tether to the device and confirm compliance with basic security policies. But that leaves a lot of room for problems. Closing that vulnerability gap requires ongoing communication to maintain security awareness and keep users from falling for increasingly sophisticated spear-phishing attacks, for example.

Many companies start out thinking that, by shifting to a BYOD model, they can save money by cutting back on support. Nope. Regardless of who owns the device, the goal of any mobility initiative is to make people more accessible and productive. If a user can't call the help desk and thus ends up blowing half a day trying to get something on his phone to work correctly, that defeats the purpose.

Our End User Device Management Survey found that organizations vary widely in their support plans for user-owned devices. Only 23% report that they encourage employees to contact tech support for assistance, while another 23% take the "sink-or-swim" approach and make it



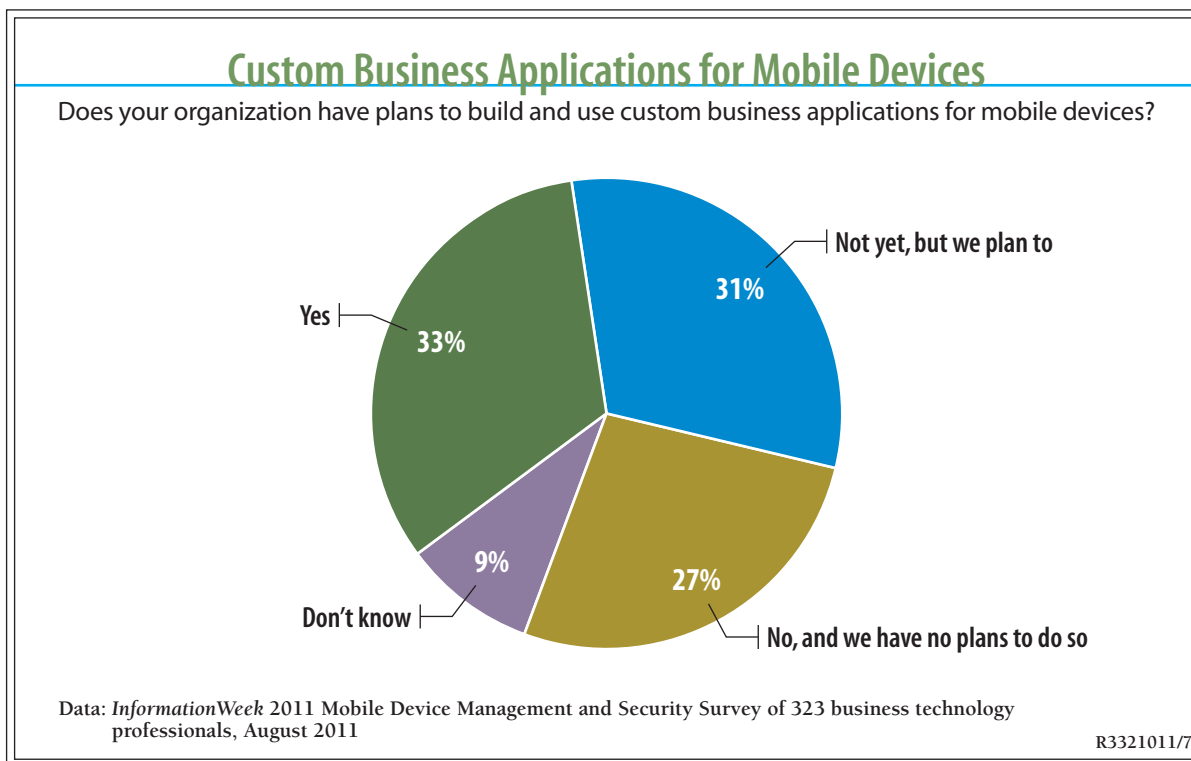
Strategy Session

clear users are on their own. Thirty-two percent report having no policy but say they help users on an ad hoc basis.

So, in planning how to make the shift to BYOD, pay great attention to defining IT's role, not only how your team will manage and secure both corporate-liable and individual-liable devices, but what services IT will provide for each population, device or platform. Just don't leave users wondering.

Applications: The biggest challenge, however, will be in applications. The overall business goal is not to accommodate personal preferences for mobile devices, though employee satisfaction typically spikes when you let people pick their own phones. The goal is to make the organization more efficient and effective through the use of mobile technologies. As long as your vision encompasses only mobile email, a personal information manager and personal productivity tools, such as the ability to view Word docs and spreadsheets on the mobile device, you'll have a lot of options to choose from.

Figure 6



**S t r a t e g y S e s s i o n**

Those out-of-the-box applications are fine for improving “individual” productivity, but the real return on mobility comes when we can incorporate mobility into line-of-business applications. Whether we develop those applications internally, outsource the coding or simply opt for the packaged mobilized software offered by independent software vendors, the range of mobile platforms supported (and we now include tablets in that calculation) will be the deciding factor. You don’t want to put your organization in a position where it can’t deploy the applications needed to transform the business because you’ve decided to support every mobile OS under the sun.

Catch Up

Mobile adoption has shot up so dramatically that, in many cases, it’s gotten ahead of IT’s ability to manage it effectively. Further, the focus on cost control and plan optimization has pushed more important issues, such as security and the potential for business transformation, to the side. With the adoption of BYOD, a failure to develop and enforce policies and plans could leave organizations floundering in an environment that impairs their ability to put these new mobile technologies to their best business use.

The advance of smartphones, tablets and other mobile devices—along with the networks to support them—has been one of the great technology stories of the past decade. However, most of that focus has been on the consumer rather than the enterprise side. As with any new technology, success comes from the ability to use it effectively in a business context. The intermixing of people’s business and personal lives has led to the intermixing of their technologies as well, but it is still incumbent on IT to protect and advance the best interests of the enterprise.

**S t r a t e g y S e s s i o n**

Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying new projects or implementing new systems, there's no substitute for experience. And that's what **InformationWeek** provides—analysis and advice from IT professionals. Our Reports site houses more than 900 reports and briefs, and more than 100 new reports are slated for release in 2011. *Right now, you'll find:*

Research: Application Mobilization: A Rapidly Changing Landscape: Mobile apps are becoming strategic tools for companies trying to make employees more efficient, better service customers and better compete in global markets. This report, we'll showcase some trends and discuss ongoing challenges.

Research: Trifecta of Change: 2011 End User Device Survey: The forces of cloud, mobility and consumerization will eventually spell the end of the fat corporate desktop. Think you can hold the line? Maybe. But the real question is, should you?

IT Pro Impact Report: Android Invasion: The Android OS is coming to your enterprise in smartphones and tablets. We provide key details for bringing Android into the IT fold, including security, Exchange integration, management and app development.

Strategy: 8 Steps to Create a Mobile App Environment: Taking your company's mobile capabilities to the next level requires a plan that encompasses development, distribution, security, support and enhancement. We show you how to get there.

Buyer's Guide: Mobile Device Management: As a greater variety of smartphones and tablets tap into corporate resources, IT must have a strategy for security, access control and management. Our buyer's guide helps you make the right call on MDM tools.

PLUS: Signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.